**Statement for the Record**
**of**
**Philip Reitinger**
**Deputy Under Secretary**
**National Protection and Programs Directorate**
**Department of Homeland Security**

**RADM Michael A. Brown, USN**
**Deputy Assistant Secretary**
**Office of Cybersecurity and Communications**
**National Protection and Programs Directorate**
**Department of Homeland Security**

**Before the**
**United States House of Representatives**
**House Appropriations Committee**
**Subcommittee on Homeland Security**
**Washington, DC**

**April 15, 2010**

## Introduction

Thank you, Chairman Price, Ranking Member Rogers, and distinguished Members of the Committee. It is a pleasure to appear before you today to discuss the Department of Homeland Security's (DHS) cybersecurity mission and related budget request. The President's Budget request for cybersecurity both supports the Department's critical mission in Fiscal Year (FY) 2011 and lays a solid foundation for the future.

Mr. Chairman, the United States confronts a dangerous combination of known and unknown vulnerabilities, strong and rapidly expanding adversary capabilities, and a lack of comprehensive threat and vulnerability awareness. Within this dynamic environment, we are confronted with threats that are more targeted, more sophisticated, and more serious.

Sensitive information is routinely stolen from both government and private sector networks, undermining confidence in our information systems, the information collection and sharing process, and the information these systems contain.

As bad as the loss of precious national intellectual capital is, we increasingly face threats that are even greater. We currently cannot be certain that our information infrastructure will remain accessible and reliable during a time of crisis.

We face persistent, unauthorized, and often unattributed intrusions to Federal Executive Branch civilian networks. These intruders may come from nation states, terrorist networks, organized criminal groups, or individuals located here in the United States. They have varying levels of access and technical sophistication, but all have nefarious intent. Many are capable of targeting

elements of the U.S. information infrastructure to disrupt, dismantle, or destroy systems upon which we depend. Motives include intelligence collection, intellectual property or monetary theft, or disruption of commerce activities, among others. Criminal elements continue to show increasing levels of sophistication in their technical and targeting capabilities and have shown a willingness to sell these capabilities on the underground market. Terrorist groups and their sympathizers have expressed interest in using cyberspace to target and harm the United States and its citizens. While some have commented on terrorists' own technical abilities, the availability of technical tools for purchase and use by others remains a serious threat.

In the virtual world of cyberspace malicious cyber activity can instantaneously result in virtual or physical consequences that threaten national and economic security, critical infrastructure, public health and welfare, and confidence in government. Similarly, stealthy intruders can lay a hidden foundation for future exploitation or attack, which they can then execute at their leisure—and at their time of greatest advantage. Securing cyberspace is similar to protecting physical borders and ports, enforcing and facilitating the immigration laws, securing the aviation and surface transportation system, and preparing to respond from both natural and manmade events simultaneously: it requires a layered security approach. Indeed, securing cyberspace is also critical to accomplishing each of these missions successfully.

In cyberspace, just as in physical domains, we need to ensure that the federal perimeter is secure and that legitimate traffic is allowed to flow freely while malicious traffic is prevented from penetrating our defenses. Further, we must use our knowledge of these systems and their interdependencies to prepare to respond should our defensive efforts fail. This is a serious challenge, and DHS is continually making strides to improve the nation's overall operational posture and forward-leaning policy efforts.

Specifically, DHS is responsible for securing the networks of the Federal Executive Branch civilian departments and agencies, often called the dot-gov domain. DHS also works closely with partners across government and in industry to assist with the protection of private sector critical infrastructure networks. The Department has a number of foundational and forward-looking efforts under way, many of which stem from the Comprehensive National Cybersecurity Initiative (CNCI).

The CNCI consists of a number of mutually reinforcing initiatives with the following major goals designed to help secure the United States in cyberspace:

- Establish a front line of defense against today's immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the federal government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.
- Defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.
- Strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the federal

government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.

DHS plays a key role in many of the activities supporting these goals and works closely with our federal partners to secure our critical information infrastructure in a number of ways. First, we are reducing and consolidating the number of external connections federal agencies have to the Internet through the Trusted Internet Connections (TIC) initiative. Further, DHS continues to deploy its intrusion detection capability, known as EINSTEIN 2, to those TICs. In addition, through the United States Computer Emergency Readiness Team (US-CERT), we are working more closely than ever with our partners in the private sector and across the federal government to share what we learn from EINSTEIN 2 and to deepen our collective understanding, identify threats collaboratively, and develop effective security responses.

President Obama determined that the CNCI and its associated activities should evolve to become key elements of the broader national cybersecurity strategy. These CNCI initiatives will play the central role in implementing many of the key recommendations of President Obama's *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*.

With the publication of the *Cyberspace Policy Review* on May 29, 2009, DHS and its components have developed a long-range vision of cyber security for the Department's and the nation's homeland security enterprise. This effort resulted in the elevation of cybersecurity to one of the Department's five priority missions, as articulated in the Quadrennial Homeland Security Review (QHSR), an overarching framework for the Department that defines our key priorities and goals and outlines a strategy for achieving them. Within the cybersecurity mission area, the QHSR details two overarching goals: to help create a safe, secure and resilient cyber environment, and to promote cybersecurity knowledge and innovation.

In alignment with the QHSR, Secretary Napolitano has consolidated the Department's cybersecurity efforts under the National Protection and Programs Directorate (NPPD). As NPPD leadership, we are moving aggressively to build a world-class cybersecurity team, and we have identified three key priorities that enable and establish a "system-of-systems" approach that encompasses the people, processes, and technologies needed to create a front line of defense and grow the nation's capacity to respond to new and emerging threats. The three key priorities are as follows:

1. Continue development of the EINSTEIN system's capabilities as a critical tool in protecting our Federal Executive Branch civilian departments and agencies.
2. Develop the National Cyber Incident Response Plan (NCIRP) in full collaboration with the private sector and other key stakeholders. The NCIRP will ensure that all national cybersecurity partners understand their roles in cyber incident response and are prepared to participate in a coordinated and managed process. The NCIRP will be tested this fall during the Cyber Storm III National Cyber Exercise.
3. Increase the security of automated control systems that operate elements of our national critical infrastructure. Working with owners and operators of the nation's critical infrastructure and cyber networks, we will continue to conduct vulnerability

assessments, develop training, and educate the control systems community on cyber risks and mitigation solutions.

These capabilities are being carefully designed in close consultation with privacy experts—protecting civil rights, civil liberties, and privacy remains fundamental to the development and deployment of cybersecurity tools.

DHS also bears primary responsibility for raising public awareness about threats to our nation's cyber systems and networks. Every October, we make a concerted effort to educate the public through the National Cybersecurity Awareness Month (NCSAM) campaign. We are making progress—in 2009, for example, all 50 states, the District of Columbia, and the U.S. Territory of American Samoa, as well as seven tribal governments, endorsed NCSAM.

Teamwork—ranging from intra-agency to international collaboration—is essential to securing cyberspace. Simply put, the cybersecurity mission cannot be accomplished by any one agency; it requires teamwork and coordination because it touches every aspect of our lives. Together, we can leverage resources, personnel, and skill sets that are needed to accomplish the cybersecurity mission. The FY 2011 NPPD budget request for cybersecurity strengthens the ongoing work in each of the Department's offices to fulfill our unified mission. I will now summarize the FY 2011 NPPD cybersecurity budget request and its associated goals.

The Office of Cybersecurity and Communications (CS&C), a component of NPPD, is focused on reducing risk to the nation's communications and IT infrastructures and the sectors that depend upon them; and enabling timely response and recovery of these infrastructures under all circumstances. CS&C also coordinates national security and emergency preparedness communications planning and provisioning for the federal government and other stakeholders. CS&C is comprised of three divisions: the National Cyber Security Division (NCSD), the Office of Emergency Communications, and the National Communications System.

NCSD collaborates with the private sector, government, military, and intelligence stakeholders to conduct risk assessments and mitigate vulnerabilities and threats to information technology assets and activities affecting the operation of the civilian government and private sector critical cyber infrastructures.

NCSD also provides cyber threat and vulnerability analysis, early warning, and incident response assistance for public and private sector constituents. To that end, NCSD carries out the majority of DHS' responsibilities under the CNCI. The FY 2011 budget request for NCSD is $378.744 million and includes 342 federal positions, continuing to fund key Administration cybersecurity programs to address and counter the threat of cyber attack.

The FY 2011 request enables NCSD to continue and build upon its accomplishments, which include:

- Activation of the National Cybersecurity and Communications Integration Center (NCCIC), a new unified operations center co-locating the watch operations of the National Coordinating Center for Telecommunications, US-CERT, and the National Cyber Security Center. NCCIC will improve the nation's capability and capacity to

detect, prevent, respond, and mitigate disruptions due to voice and cyber communications risks.

- Sponsored the sixth NCSAM campaign, which promoted cybersecurity initiatives that ensure the confidentiality of sensitive information, the integrity of e-commerce, and the resiliency of digital infrastructures.
- Finished FY 2009 ahead of schedule for EINSTEIN 2 deployments - deploying EINSTEIN 2 to nine TIC Access Providers and three Managed Trusted Internet Protocol Service (MTIPS) vendors, exceeding the goals for deployments of five to TIC Access Providers and two to MTIPS vendors. EINSTEIN 2 has provided DHS with an unprecedented level of visibility into malicious activity happening within the federal executive branch civilian networks.
- Completed eight Trusted Internet Connections Compliance Validation assessments in FY 2009, surpassing the goal of six.
- Facilitating the release of the CNCI Initiative 3 Exercise Privacy Impact Assessment on March 18, 2010.
- Conducted tabletop exercises on November 20, 2009, February 18 & 26, 2010, testing the draft NCIRP, including incident response procedures and communications.
- Launched, on February 19, 2010, in partnership with the Department of Defense (DOD) and the Financial Services Information Sharing and Analysis Center, a pilot program that enables the bi-directional sharing of cybersecurity information.
- Conducted a mid-term planning conference for Cyber Storm III, the biennial national level exercise that brings together Federal, State, international, and private sector partners to assess participants' response and coordination capabilities in response to a cyber incident. Cyber Storm III will take place this fall.
- Launched, with the State of Michigan, a proof of concept that leverages federally developed cybersecurity technology at the state level. DHS deployed a network flow monitor technology, EINSTEIN 1, to detect anomalous behavior on the State of Michigan's networks managed by their executive branch.
- Initiated a pilot and implementation, together with private sector partners, of the Cybersecurity Partners Local Access Plan (CPLAP), which will allow owners and operators of CIKR to access cybersecurity information at their local fusion centers. The CPLAP will allow private sector partners with the necessary security clearances to access to Secret-level classified information, and creates a forum for DHS to conduct multi-directional information sharing for threat context, vulnerability identification and analysis, and consequence discussion across CIKR sectors and levels of government.

NCSD is funded through the following three Congressionally appropriated Programs, Projects and Activities (PPA): US-CERT, Strategic Initiatives, and Outreach and Programs.

**PPA #1: US-CERT**

US-CERT leverages technical competencies in federal network operations and threat analysis centers to develop knowledge and knowledge management practices. US-CERT provides a single, accountable focal point to support federal stakeholders as they make key operational and implementation decisions and secure the Federal Executive Branch civilian networks. It does so through a holistic approach that enables federal stakeholders to address cybersecurity challenges in a manner that maximizes value while minimizing risks associated with technology and

security investments. Further, US-CERT analyzes threats and vulnerabilities, disseminates cyber threat warning information, and coordinates with partners and customers to achieve shared situational awareness related to the Nation's cyber infrastructure.

US-CERT funds also support the development, acquisition, deployment, and personnel required to implement the National Cybersecurity Protection System (NCPS), operationally known as EINSTEIN. The EINSTEIN Program is an automated intrusion detection system for collecting, correlating, analyzing, and sharing computer security information across the federal government to improve our Nation's situational awareness. EINSTEIN is an early warning system that monitors the network gateways of Federal Executive Branch civilian departments and agencies for malicious cyber activity.

DHS is deploying EINSTEIN 1 and 2 systems in conjunction with the federal TIC initiative, which optimizes network security capabilities into a common solution for the Federal Executive Branch and facilitates the reduction and consolidation of external connections, including Internet points of presence, through approved access points.

| | FY 2010 Enacted | | FY 2011 Request | | FY 2011 - FY2010 Change | |
|---|---|---|---|---|---|---|
| | POS | $000 | POS | $000 | POS | $000 |
| **US-CERT** | **207** | **$ 323,629** | **288** | **$ 314,989** | **81** | **$ (8,640)** |
| US-CERT Salaries & Benefits | 207 | $ 20,342 | 229 | $ 28,856 | 22 | $ 8,514 |
| Cybersecurity Coordination Salaries & Benefits | | $ - | 40 | $ 4,181 | 40 | $ 4,181 |
| AS CS&C Salaries & Benefits | | $ - | 19 | $ 3,995 | 19 | $ 3,995 |
| **Program Costs** | | **$ 303,287** | | **$ 277,957** | | **$ (25,330)** |
| Cybersecurity Coordination | | $ 5,000 | | $ 5,819 | | $ 819 |
| Incident Handling | | $ 15,257 | | $ 14,213 | | $ (1,044) |
| Analysis | | $ 27,416 | | $ 21,748 | | $ (5,668) |
| Strategic Operations | | $ 14,701 | | $ 14,193 | | $ (508) |
| Situational Awareness (includes Data Center) | | $ 232,689 | | $ 213,897 | | $ (18,792) |
| Production | | $ 8,224 | | $ 7,836 | | $ (388) |
| AS CS&C | | $ - | | $ 251 | | $ 251 |

Table 1: US-CERT Funding

DHS requests $314.989 million for US-CERT in FY 2011, which includes 288 federal positions, continuing a steady increase in federal employee staffing in the budget request year-over-year. These positions are a mix of new positions and positions funded by reductions in program/contract dollars. The FY 2011 request includes a $9.528 million enhancement, including 11 federal positions, to implement an assessment, testing, and analysis capability that tests and measures Federal Executive Branch civilian departments' and agencies' compliance with laws, regulations, policies, and standards relating to information security. There is a program reduction of $13.282 million from EINSTEIN 3 deployment to account for cost and schedule uncertainties. Other FY 2011 reductions include non-recurring costs such as the $8 million for data center migration and a $4 million transfer for the National Computer Forensics Institute funding to the Federal Law Enforcement Training Center.

In addition, $10 million for the National Cyber Security Center (NCSC) is requested under US-CERT's budget. The NCSC fulfills its presidential mandate as outlined in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 in ensuring that federal agencies can access and receive information and intelligence needed to execute their respective

cybersecurity missions. The NCSC accomplishes this through the following six mission areas: Mission Integration, Collaboration and Coordination, Situational Awareness and Cyber Incident Response, Analysis and Reporting, Knowledge Management, and Technology Development and Management, each supported by developing NCSC programs and capabilities.

*FY 2011 Activities*

In FY 2011, US-CERT intends to:

- Continue to conduct analysis and coordinate both defense and response support against cyber attacks.
- Continue managing the Trusted Internet Connection (TIC) Initiative through activities that will result in federal enterprise network connection reductions and consolidations.
- Through the new Assessment, Testing, and Analysis Capability (ATAC), perform 27 red team/blue team compliance assessments to support TIC Initiative implementation and cybersecurity mandate compliance.
- Refine resource requirements for the initial deployment of EINSTEIN 3 to meet updated timelines for key deliverables. NPPD will provide this Committee with regular updates on progress.
- Maintain collaboration with the Department of Defense (DOD), the National Institute of Standards and Technology (NIST), and other leading federal departments and agencies to continue leadership of the CNCI Education Initiative.
- Provide a gap analysis of existing policy and guidance for supply chain risk management across high priority national security and federal government systems, and recommend corrective steps as needed.

In FY 2011, NCSC plans to:

- Measure and report effectiveness of integration, collaboration, and information sharing among the six largest federal cybersecurity centers.
- Expand reporting on significant national cyber incidents.
- Implement the Knowledge Management System with data enriching features focused on raising common situational awareness.
- Support and integrate incident response activities under the NCIRP.
- Co-lead efforts of CNCI Initiative 5 to build processes, policies, and tools to enable integrated operational actions with the six federal cybersecurity centers.

**PPA #2: Strategic Initiatives**

Strategic Initiatives enables NCSD to establish mechanisms for federal partners to deploy standardized tools and services at a reduced cost, paving the way for a collaborative environment that enables the sharing of best practices and common security challenges and shortfalls. In addition, Strategic Initiatives enables NPPD to develop and promulgate sound practices for software developers, IT security professionals, and other CIKR stakeholders; it also enables collaboration with the public and private sectors to assess and mitigate risk to the nation's cyber CIKR.

| | FY 2010 Enacted | | FY 2011 Request | | FY 2011 - FY2010 Change | |
|---|---|---|---|---|---|---|
| | POS | $000 | POS | $000 | POS | $000 |
| **Strategic Initiatives** | **37** | **$ 64,179** | **38** | **$ 56,880** | **1** | **$ (7,299)** |
| SI Salaries & Benefits | 37 | $ 3,943 | 38 | $ 4,024 | 1 | $ 81 |
| **Program Costs** | | **$ 60,236** | | **$ 52,856** | | **$ (7,380)** |
| Critical Infrastructure Protection | | $ 12,452 | | $ 8,713 | | $ (3,739) |
| Training & Education | | $ 5,847 | | $ 1,365 | | $ (4,482) |
| Software Assurance | | $ 2,641 | | $ 2,510 | | $ (131) |
| Cyber Exercises | | $ 3,701 | | $ 7,102 | | $ 3,401 |
| Standards & Best Practices | | $ 6,431 | | $ 3,295 | | $ (3,136) |
| ISS Line of Business | | $ 2,600 | | $ 2,600 | | $ - |
| Control Systems | | $ 26,564 | | $ 27,258 | | $ 694 |
| AS CS&C | | $ - | | $ 13 | | $ 13 |

Table 2: Strategic Initiatives Funding

In FY 2011, NPPD requests $56.880 million for Strategic Initiatives, which includes 38 federal positions. This request includes a $3.283 million enhancement to program funding to increase the number of cyber exercises supported and conducted with stakeholders as well as technical assistance and training sessions. The request also includes a $3.700 million enhancement to enable mission critical activities, which includes support for site assistance visits with state, local, and private sector partners to identify vulnerabilities and mitigation strategies.

*FY 2011 Activities*

In FY 2011, Strategic Initiatives include:

- Participating in federal government-wide cybersecurity initiatives and serving as an information conduit to promote collaboration in providing e-government services and share lessons learned.
- Co-sponsoring software security automation and measurement capabilities with DOD, NIST, and the National Security Agency.
- Participating in and providing technical expertise to various cybersecurity standards committees.
- Maintaining interagency cybersecurity training partnerships to share investment and increase availability of shared training and experiential learning resources across the federal government.
- Expanding the Control Systems Security Program (CSSP) Industrial Control Systems Cyber Emergency Response Team's (ICS-CERT), Advanced Vulnerability Discovery facility with improved technologies.
- Maintaining an ongoing program review, enhancement, and distribution of the Cyber Security Evaluation Tool across the control systems community.
- Conducting 75 Cyber Resiliency Reviews of CIKR sites.
- Evaluating the results of the Cyber Storm III National Cyber Exercise.

**PPA #3: Outreach and Programs**

Outreach and Programs promotes opportunities to leverage the cybersecurity investments of public and private industry partners. This PPA encourages cybersecurity awareness among the

general public and within key communities, maintains relationships with government cybersecurity professionals to share information about cybersecurity initiatives, and develops partnerships to promote collaboration on cybersecurity issues. Outreach and Programs enables governance and assistance in setting policy direction and establishes resource requirements for NCSD's complex activities.

| | FY 2010 Enacted | | FY 2011 Request | | FY 2011 - FY2010 Change | |
|---|---|---|---|---|---|---|
| | POS | $000 | POS | $000 | POS | $000 |
| **Outreach and Programs** | **16** | **$ 9,346** | **16** | **$ 6,875** | **-** | **$ (2,471)** |
| O&P Salaries & Benefits | 16 | $ 1,935 | 13 | $ 1,496 | (3) | $ (439) |
| AS CS&C Salaries & Benefits | | $ - | 3 | $ 485 | 3 | $ 485 |
| **Program Costs** | | **$ 7,411** | | **$ 4,894** | | **$ (2,517)** |
| Stakeholder Outreach, Communication & Coordination | | $ 3,592 | | $ 3,336 | | $ (256) |
| International Affairs & Public Policy | | $ 653 | | $ 656 | | $ 3 |
| Planning & Programs | | $ 916 | | $ 902 | | $ (14) |
| Information Sharing & Collaboration | | $ 2,250 | | $ - | | $ (2,250) |
| AS CS&C | | $ - | | $ - | | $ - |

Table 3: Outreach and Programs Funding

In FY 2011, NPPD requests $6.875 million for Outreach and Programs, a decrease of $2.471 million from the previous year, and authority to create 16 federal positions. The Outreach and Programs FY 2011 request includes a reduction of $2.250 million for an Information Sharing and Collaboration project. This will not jeopardize the program mission or objectives, and the Information Sharing and Collaboration project will meet requirements and goals with the funding provided.

*FY 2011 Activities*

In FY 2011, Outreach and Programs activities include:

- Sponsoring the seventh annual National Cybersecurity Awareness Month in October 2011 and arranging a host of multi-media information, activities, and events to inform and educate the general public, government and private sector partners, and the international community about cyber threats and mitigation.
- Further advance state, local and international collaboration and coordination through Department engagements including the Multi-State Information Sharing and Analysis Center, the National Association of State Chief Information Officers, state and local fusion centers, the National Governors Association (NGA), and the NGA State Homeland Security Advisors Council.
- Enhance NCSD transparency and efficiency by the continued implementation of governance, protocols, and standard procedures, including process improvements that reduce the time required to develop and process procurement requests, which will improve budget execution.

**NCSD Budget Structure**

In order to increase visibility and transparency into how NCSD is executing mission requirements, NPPD proposes a new budget structure to be implemented beginning in FY 2011, permitting NCSD to better align appropriated resources with its responsibilities. Changing the

NCSD budget structure will also provide a structure that is congruent with NPPD's finance and accounting processes.

The requested budget structure for NCSD fulfills the mission requirements through its five operational units and a supporting business operational project.

Specifically, the proposed budget structure included two PPAs: Cybersecurity and Cybersecurity Coordination.

1. The Cybersecurity PPA will consist of US-CERT Operations; Federal Network Security; Network Security Deployment; Global Cyber Security Management; Critical Infrastructure Cyber Protection and Awareness; and Business Operations. This is the National Cyber Security Division.
2. The Cybersecurity Coordination PPA will consist of mission integration; collaboration and coordination; situational awareness and cyber incident response; analysis and reporting; knowledge management; and technology and development management. This is the National Cyber Security Center.

**Conclusion**

Chairman Price, Ranking Member Rogers, and distinguished Members of the Subcommittee, let us end by thanking you for the strong support you have provided the Department this past year. Cybersecurity is a serious challenge, and DHS is continually making strides in improving the capabilities of the national homeland security enterprise. The FY 2011 budget continues efforts to use our resources as efficiently and effectively as possible. We are exercising strong fiscal discipline, making sure that we are investing our resources in what works, increasing transparency, eliminating ineffective programs, and making improvements across the board.

Our objective is to strengthen efforts that are critical to the nation's security, bolster the Department's ability to combat terrorism and respond to emergencies and potential threats, and allow DHS to tackle its responsibilities to protect the nation and keep Americans safe.

Thank you for again for this opportunity to testify. We would be happy to answer any of your questions.